ANAMNÈSE • SMSI

SENSIBILISATION
SÉCURITÉ INFORMATIQUE

Date : **01/07/2026**

Version : **V1.0**

DIFFUSION INTERNE

Sommaire

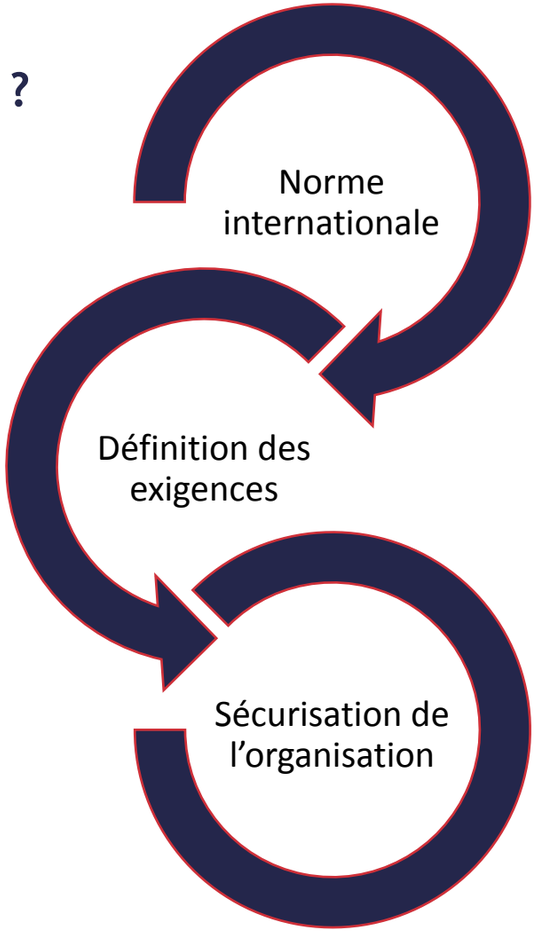
ISO 27001 HDS

ISO 27001 HDS

QU'EST-CE QUE L'ISO 27001

QU'EST-CE QUE L'ISO 27001 ?

Elle définit les exigences pour la mise en place d'un Système de Management de la Sécurité de l'Information (SMSI).



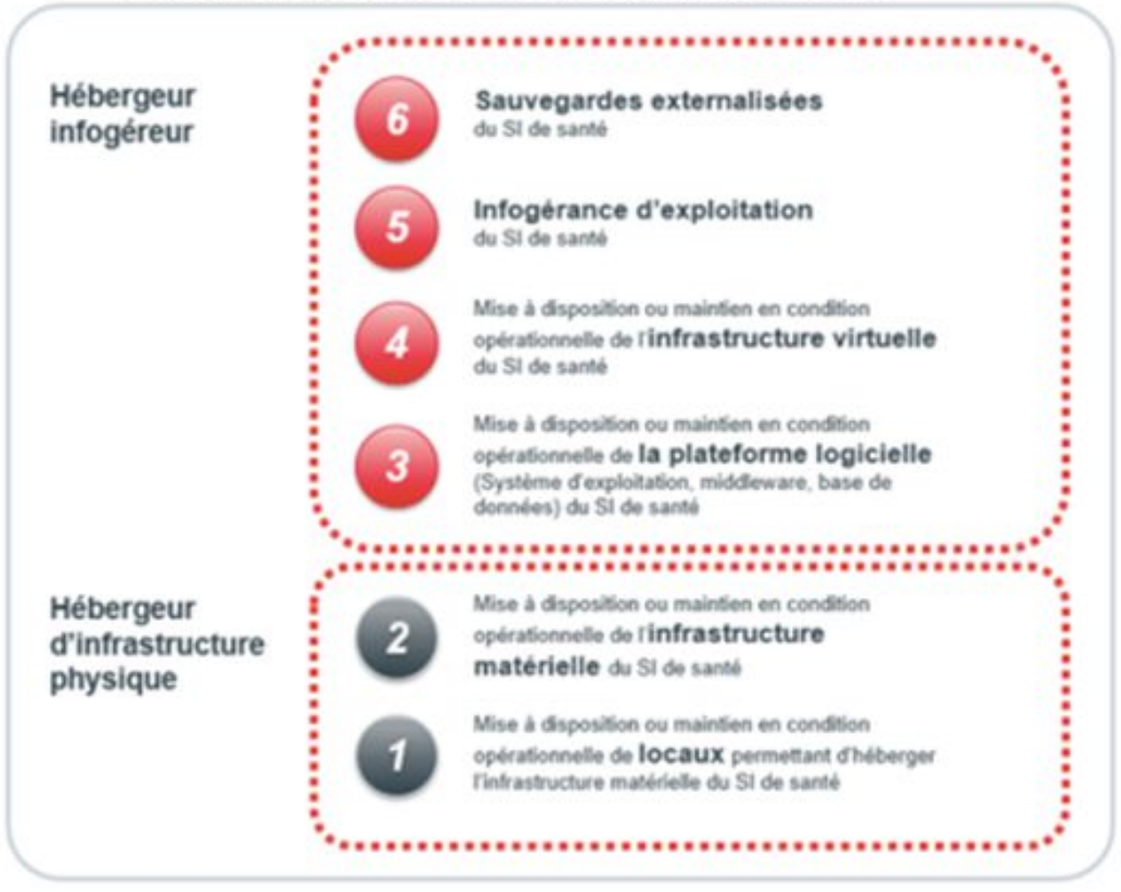
L'objectif est de protéger les informations de ANAMNESE et de ses clients de toute perte, vol ou altération de données.

ISO 27001 HDS

QU'EST-CE QUE LE HDS

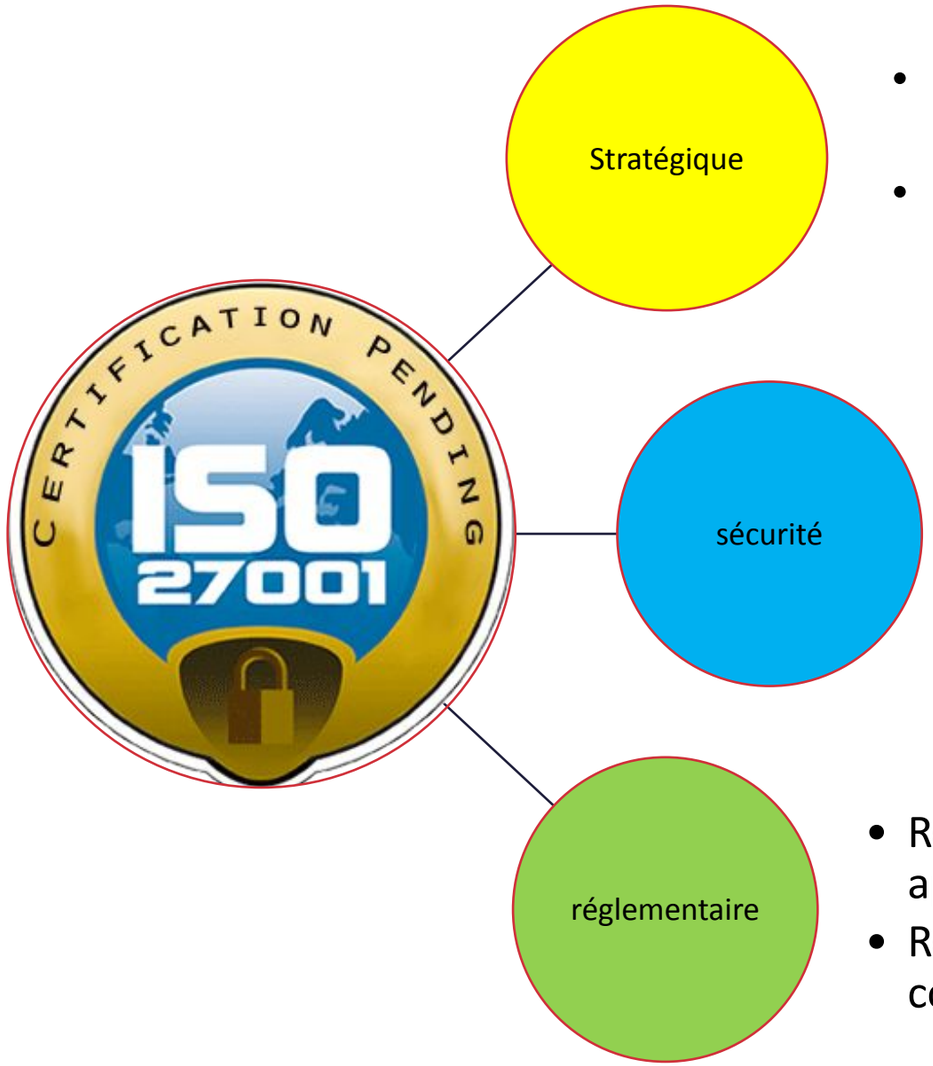
Une ISO 27001 surchargée

1 certification et 2 certificats



ISO 27001 HDS

LES ENJEUX



- Acquérir de nouveaux marchés
- Rester compétitif

- Garantir la sécurité des données de ANAMNESE et ses clients

- Respect de la réglementation applicable (RGPD)
- Respect de nos clauses contractuelles (NIS2)

ISO 27001 HDS

DÉROULEMENT DU CYCLE

DATE INITIALE

Audit initial et Renouvellement

Obtention du certificat pour un cycle de 3 ans.

+ 1 AN

Audit de suivi 1

Maintien & Évolution du SMSI

Vérification annuelle de l'efficacité et de l'amélioration continue du système de management.

+ 2 ANS

Audit de suivi 2

Maintien & Évolution du SMSI

Deuxième surveillance avant l'audit de renouvellement de l'année 3.

ISO 27001 HDS

PÉRÈMETRE DE CERTIFICATION

DANS LE PÉRIMÈTRE (CERTIFIÉ)

Activités Opérationnelles

- **Build & Run :** Cycle de vie complet de la plateforme SaaS ANAMNESE (conception, dév, intégration, déploiement)
- **Support & Exploitation :** Maintien en condition de sécurité et d'opération
- **Hébergement :** Infrastructures de production cloud certifiées HDS

Fonctions Support & Gouvernance

- **Gouvernance :** Direction Générale, DSI et RSSI
- **Processus Support :** Patrimoine Humain, Administratif & Financier, Architecture

HORS PÉRIMÈTRE

Fonctions Exclues

- **Marketing & Communication :** Non inclus dans le périmètre direct de certification
- **Commerce :** Activités d'avant-vente et commerciales

Infrastructures Hors Périmètre

- **Équipements clients :** Terminaux et réseaux locaux propres aux clients
- **Applications tierces :** Solutions opérées en dehors de ANAMNESE

** Note : Bien qu'exclus du périmètre certifié, l'intégralité des collaborateurs reste soumise à l'application des politiques du SMSI et aux actions de sensibilisation.*

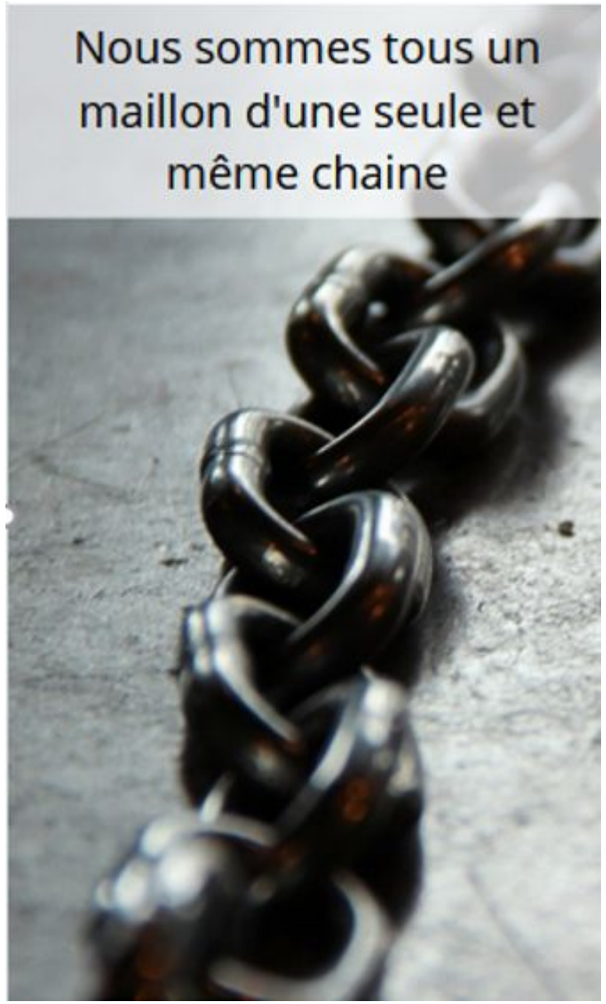
ISO 27001 HDS

QUI EST CONCERNÉ

TOUT LE MONDE :

NOUS SOMMES TOUS UN MAILLON DE LA CHAÎNE

Une chaîne est aussi solide que son maillon le plus faible



2 types de non-conformité

NON-CONFORMITÉ MINEURE

- 1 AN POUR LES CORRIGER
- PLUSIEURS NON-CONFORMITÉS MINEURES PEUVENT MENER À UNE MAJEURE

NON-CONFORMITÉ MAJEURE

- 2 SEMAINES POUR LES CORRIGER
- PEUT MENER À LA PERTE DE LA CERTIFICATION EN CAS DE NON-RÉSOLUTION DE LA NC

GESTION DOCUMENTAIRE

- Décrit le cycle de vie des documents
  - **Création**
    - Modèles de document
    - Cartouche à respecter
  - **Diffusion & Mise à jour**
    - Informer les personnes concernées
  - **Stockage et accès**
    - Stocker les fichiers sur le réseau avec les bons droits d'accès associés

CLASSIFICATION DES DOCUMENTS

Objectif : Déterminer le niveau de sensibilité du document en fonction de l'impact en cas de divulgation de la donnée afin d'adapter son niveau de protection.

- 3 niveaux de classification :
  - PUBLIC : Données ou informations pouvant être divulguées au public sans impact pour les activités de ANAMNESE (ex : informations sur notre site web, info données dans des salons, etc…)
  - INTERNE : Données ou informations à faible impact sur les activités de ANAMNESE en cas de divulgation. (ex : PGSSI, procédures génériques, documents pour certains prospect, etc…)
  - CONFIDENTIEL : Données ou informations ayant des impacts importants pour les activités de ANAMNESE (ex: perte d'image ou de client) en cas de divulgation. (ex : Données client, données de santé, documents techniques type schéma réseau, documents stratégiques, contrats client, analyse de risque, etc..)

DÉLAIS DE NOTIFICATION (Service ISI)

RÉGLEMENTATION RGPD / NIS2

Notification aux clients en cas d'incidents majeurs ou violation de données à caractère personnel et de santé

- Délais :
  - Données personnelles (RGPD) : Une déclaration à la CNIL doit être faite par le propriétaire de la donnée dans les 72h suivant l'incident.
  - Incident majeur (NIS2): Une déclaration à l'ANSSI doit être faite par le propriétaire de la donnée dans les 24h suivant l'incident.
- A savoir :
  - Si la donnée appartient au client (ex : données patient) : c'est au client de faire la déclaration
  - Si la donnée appartient à ANAMNESE (ex : carte d'identité des collaborateurs), c'est à ANAMNESE de faire la déclaration

La procédure à suivre est définie dans la procédure de gestion des incidents de sécurité.

ISO 27001 HDS

PROTECTION DES DONNÉES (Service ISI)

CONFIDENTIALITÉ :

ANAMNESE ne doit pas accéder aux données du client, dont les données de santé à caractère personnel, sauf sur demande écrite du client, dans le cadre de sa mission (ex : restauration d'un fichier)

Toute donnée appartenant aux clients doit être traitée comme **confidentiel**, notamment données de santé à caractère personnel (DSCP)

INTÉGRITÉ :

ANAMNESE est garant de l'intégrité des données de ses clients, dont les DSCP. Quelques mesures pour garantir leur protection :

- Sauvegarde des données à 2 endroits différents
- Des contrôles d'accès sont mis en place
- Sensibilisation des utilisateurs

ISO 27001 HDS

PROTECTION DES DONNÉES

OBJECTIF DE DISPONIBILITÉ

99,9 %

Sur une période de 30 jours

Équivalent à un maximum de **43 minutes** d'indisponibilité glissante.

Gestion PCA-PRA

Plateforme Commune : Compte tenu de l'architecture monolithique de la solution, ANAMNESE propose un niveau de service unifié pour l'ensemble des services applicatifs.

Mesure & Transparence : La disponibilité est mesurée de manière indépendante via l'outil **UptimeRobot**. Page météo publique :

status.anamnese.care

GESTION DES CHANGEMENTS

- Définition : Un changement a pour objectif de modifier, créer ou supprimer un des composants du SI pour en améliorer la fiabilité, en renforcer la sécurité ou pour ajouter un service

- 3 types de changements

STANDARD

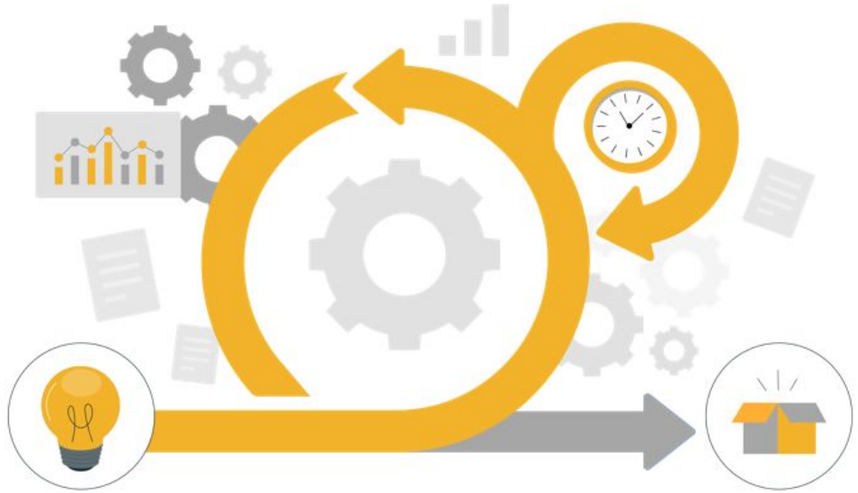
- Cadré
- Doit être tracé
- Approbation automatique

NON STANDARD

- Cadré / Non Cadré
- Doit être tracé
- Approbation nécessaire

URGENT

- Cadré / Non Cadré
- Doit être tracé
- Approbation nécessaire
- Répond à un incident de disponibilité ou de sécurité



SÉLECTION ET ÉVALUATION DES FOURNISSEURS

- Chaque nouveaux service / outils doit être contrôlé par le RSSI / DSI afin de valider la conformité de ces derniers avec nos politiques de sécurité internes (RGPD, sauvegardes, journalisation, SLA, etc.).

MISE À JOUR ET CONTRÔLE DES FOURNISSEURS

- Réception d'un email tous les 4 mois pour rappel et contrôle en cas d'oubli
- Contrôle annuel des fournisseurs sur les critères suivants :
  - La réputation
  - Le respect des SLA
  - Le maintien de certification (pour les fournisseurs critiques)
  - Le scoring bancaire (pour les fournisseurs critiques)

BASE DOCUMENTAIRE

Vous pouvez retrouver l'ensemble de la base documentaire sur Google Workspace dans le dossier :

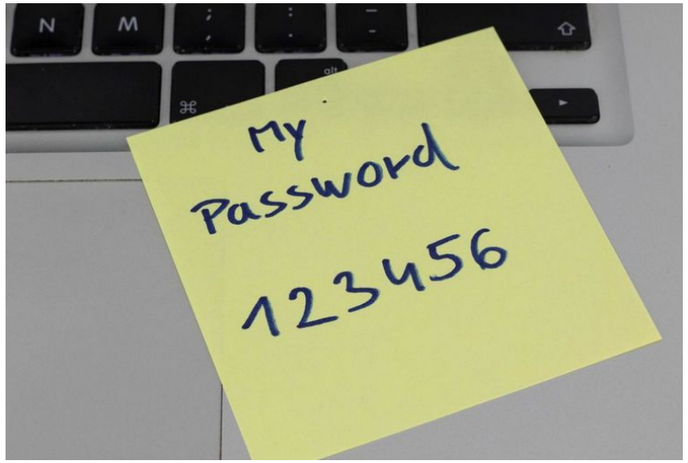
8-Formation+Méthodes+Outils \ **Politiques de sécurité**

BONNES PRATIQUES

BONNES PRATIQUES

MOTS DE PASSE

BONNES PRATIQUES DE SÉCURITÉ



- Ne pas le partager/prêter
- Ne pas les stocker dans un fichier
- Ne pas l'écrire sur un papier/post-it
- Utilisez des mots de passe complexes :

  Minimum 12 caractères, au moins une majuscule, une minuscule, un chiffre et un caractère spécial.

  Minimum 16 caractère pour les comptes administrateurs, à privilèges ou de service
- Ne pas enregistrer les mots de passe dans le navigateur.
  - Utiliser notre gestionnaire de mot de passe sécurisé (Passwordstate)
- Utiliser un mot de passe différent pour chaque site ou service (**surtout pour votre boite mail**)
- Ne pas utiliser les mêmes mots de passe personnel et professionnel.
- On ne met pas le nom de l'entreprise, ni de code postal dans ses mots de passe

BONNES PRATIQUES DE SÉCURITÉ

Les Emails

- Ne pas utiliser sa boite mail professionnelle pour une utilisation personnelle (et inversement)
- Prendre garde aux mails douteux, surtout s'ils possèdent une pièce jointe ou des liens web
- Contrôler les signaux d'alerte :
  - ATTENTION: Cet e-mail provient d'une personne externe à votre organisation. Ne cliquez pas sur les liens ou n'ouvrez pas les pièces jointes si vous ne connaissez pas l'expéditeur et que vous n'êtes pas sûr que le contenu est sûr.
  - [redacted]
    TR: [EXTERNE] Complétée : Complétez avec Docusign : Devis 2025-0...
- Eviter d'envoyer un login et mot de passe dans le même mail. Privilégier l'envoi du mot de passe par SMS ou bien via VaultWarden

BONNES PRATIQUES DE SÉCURITÉ

La navigation internet

- Ne pas naviguer sur des sites potentiellement dangereux (téléchargement de films/musiques, sites porno, conversion de format de fichier en ligne, envoi de fichiers volumineux (wetransfert, etc..))
  - envoie de fichiers : https://vault.anamnese.care

- Privilégier les sites sécurisés en HTTPS (les sites en HTTP envoient les mots de passe en clair sur le réseau)

BONNES PRATIQUES DE SÉCURITÉ

Poste de travail ANAMNESE

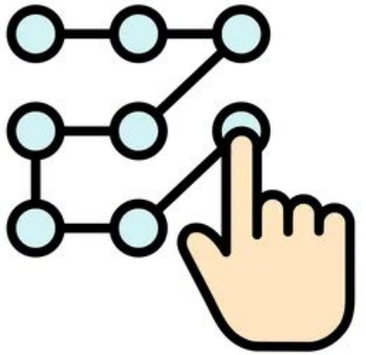
- Verrouiller le poste lorsque vous n’êtes plus devant
- Mettre régulièrement à jour votre système d’exploitation et vos logiciels.
- Ne jamais installer de logiciels piratés ou non validé dans le catalogue ANAMNESE.

TÉLÉPHONE PORTABLE

BONNES PRATIQUES DE SÉCURITÉ

Smartphone

- Sécuriser le téléphone avec un mot de passe ou un schéma au démarrage.
  - Celui-ci est différent du code PIN (lié à la carte SIM)
- Ne pas laisser des personnes tierces (enfants…) installer des jeux ou applications.
- Ne jamais installer d'applications venant de sources inconnues ou de store non officiel.
- Les données professionnelles doivent se limiter aux mails et à l'utilisation de Teams et à l'authenticator



BONNES PRATIQUES DE SÉCURITÉ

Supports amovibles

- Ne jamais brancher un câble USB, une clef USB ou un disque dur externe venant d'une source inconnue.
- Ne pas utiliser les bornes de rechargement publiques via port USB
- Ne pas brancher de clef USB personnelle sur votre poste professionnel et inversement.
- En cas de perte de support USB, prévenir le support : support@anamnese.care

SÉPARATION DOMAINES PERSONNELS & PROFESSIONNELS

BONNES PRATIQUES DE SÉCURITÉ

Personnel OU Professionnel

- Le poste doit servir exclusivement à **utilisation professionnelle**
- Son matériel est **individuel** et ne doit pas être prêté à une personne tierce comme un membre de sa famille
- Il est interdit de synchroniser ses comptes personnels sur le poste professionnel comme par exemple ses favoris de navigateurs, ses fichiers Onedrive/google drive/Dropbox/icloud/etc.

BONNES PRATIQUES

TÉLÉTRAVAIL & SITES DISTANTS

- Ne pas laisser son poste dans un endroit non sécurisé (voiture, à la vue des passants, etc…)
- Attacher votre poste avec un câble antivol dans les environnements non sécurisés (salons, etc…)
- Mettre un filtre écran de confidentialité.

TRAVAIL DEPUIS L'ÉTRANGER

- Le matériel ne doit pas être transporté en dehors des endroits autorisés par ANAMNESE (bureau, domicile).
- En cas de besoin (ex : télétravail dans un pays étranger), une autorisation écrite doit être faite par ANAMNESE.

Utilisation du WIFI lors de déplacement

L'utilisation de **WIFI public** n'est pas recommandée (Hôtel, aéroport, wifi public divers…)

En cas de besoin de connexion internet lors de déplacement, il est préférable d'utiliser par ordre de priorité :

1) Un partage de connexion avec son téléphone professionnel

2) Un partage de connexion avec son téléphone personnel

SÉCURITÉ ET PROTECTION DU MATÉRIEL À DOMICILE

Règles de sécurité au domicile & à distance

Afin d'éviter tout accès non autorisé à vos équipements de travail et de préserver la confidentialité des données d'ANAMNESE :

- **Rangement sécurisé :** L'ordinateur doit être rangé dans un endroit sûr afin d'éviter qu'il soit accessible à d'autres personnes (famille, visiteurs, etc.).
- **Pièce verrouillable :** Si possible, ranger ou utiliser l'ordinateur dans une pièce verrouillable, surtout en cas d'absence prolongée.
- **Discrétion visuelle :** Ne pas exposer le matériel à la vue depuis l'extérieur (fenêtres, balcons), pour réduire les risques de vol.

STOCKAGE ET SÉCURISATION DES POSTES DE TRAVAIL

Règles de sécurité hors en fin de journée

Afin de garantir la confidentialité et de réduire les risques de vol ou de fuite d'informations au sein de notre bureau :

- **Rangement des postes :** Ne laissez pas votre ordinateur portable ou vos équipements sur votre bureau de manière visible. Ranger impérativement votre matériel dans les armoires sécurisées prévues à cet effet.
- **Documents sensibles :** Aucun document papier contenant des données confidentielles ou internes ne doit rester accessible. Rangez et masquez toutes vos documentations sensibles dans nos étagères et meubles fermés.
- **Fermeture à clef :** Assurez-vous que les caissons, étagères et armoires de stockage sont verrouillés avant votre départ.

Nos étagères et armoires de rangement dédiées pour sécuriser vos postes et documents sensibles en fin de journée

CADRE D'USAGE DES COMPAGNONS IA

Règles de sécurité pour l'IA Grand Public

L'utilisation des IA est cadrée par la charte sur les IA se trouvant dans le partage RH. Les outils tels que ChatGPT, Grok ou Copilot ne garantissent pas la confidentialité des données ni le RGPD :

- **Interdiction des données réelles :** Ne jamais insérer de données sensibles (noms propres, secrets techniques, codes, logs ou informations internes).
- **Anonymisation stricte :** Toutes les informations identifiantes ou confidentielles doivent être impérativement retirées.
- **Utilisation de données fictives :** Remplacez systématiquement vos variables, noms et clés par des exemples fictifs ou du faux texte ("fakes") avant de soumettre vos prompts.

Exemple concret de prompt conforme

❌ **Mauvaise pratique (Données réelles)**

*"Rédige un compte-rendu de la réunion d'hier avec **Jean Dupont** (**jean.dupont@hopital.fr**) concernant l'intégration de Citana pour le **CHU de Bordeaux**."*

✅ **Bonne pratique (Anonymisation & Fictif)**

*"Rédige un compte-rendu de la réunion d'hier avec **[NOM]** (**[EMAIL]**) concernant l'intégration de Citana pour **[ÉTABLISSEMENT]**."*

Les variables sensibles sont remplacées par des balises génériques avant soumission.

DÉPÔT DES DOCUMENTS SENSIBLES OU CONFIDENTIELS

Lors du dépôt de documents sensibles, il est important de se poser les bonnes questions :

- Est-il vraiment nécessaire de le conserver ?
- Puis-je supprimer ou anonymiser certaines données ?
- Existe-t-il déjà une version officielle stockée ailleurs ?
- Est-ce le bon espace documentaire ?
- Les droits sont-ils limités au strict nécessaire ?

MENACES CYBER

UNE FORTE AUGMENTATION DES ATTAQUES CYBER DEPUIS 2024

Rançongiciel : + 255%

Phishing : + 600%

Usurpation d'identité : 41%

Quels impacts ?

- Détournement d'argent
- Mauvais traitement des patients hospitalisés
- Perte/divulgation de données
- Mauvaise image de l'entreprise
- Arrêt de l'activité

LES ATTAQUES LES PLUS FRÉQUENTES

PHISHING (HAMEÇONNAGE)

Consiste à l'envoi en masse de mails contenant des logiciels malveillants ou des liens vers des sites piégés

Comment s'en protéger :

- Ne jamais ouvrir de mail venant d'un expéditeur inconnu
- Ne pas ouvrir les pièces jointes et ne pas cliquer sur les liens
- Se rendre sur le site à partir de vos favoris ou d'une recherche sur Google
- Demander au service informatique en cas de doute

MENACES CYBER

Les reconnaître :

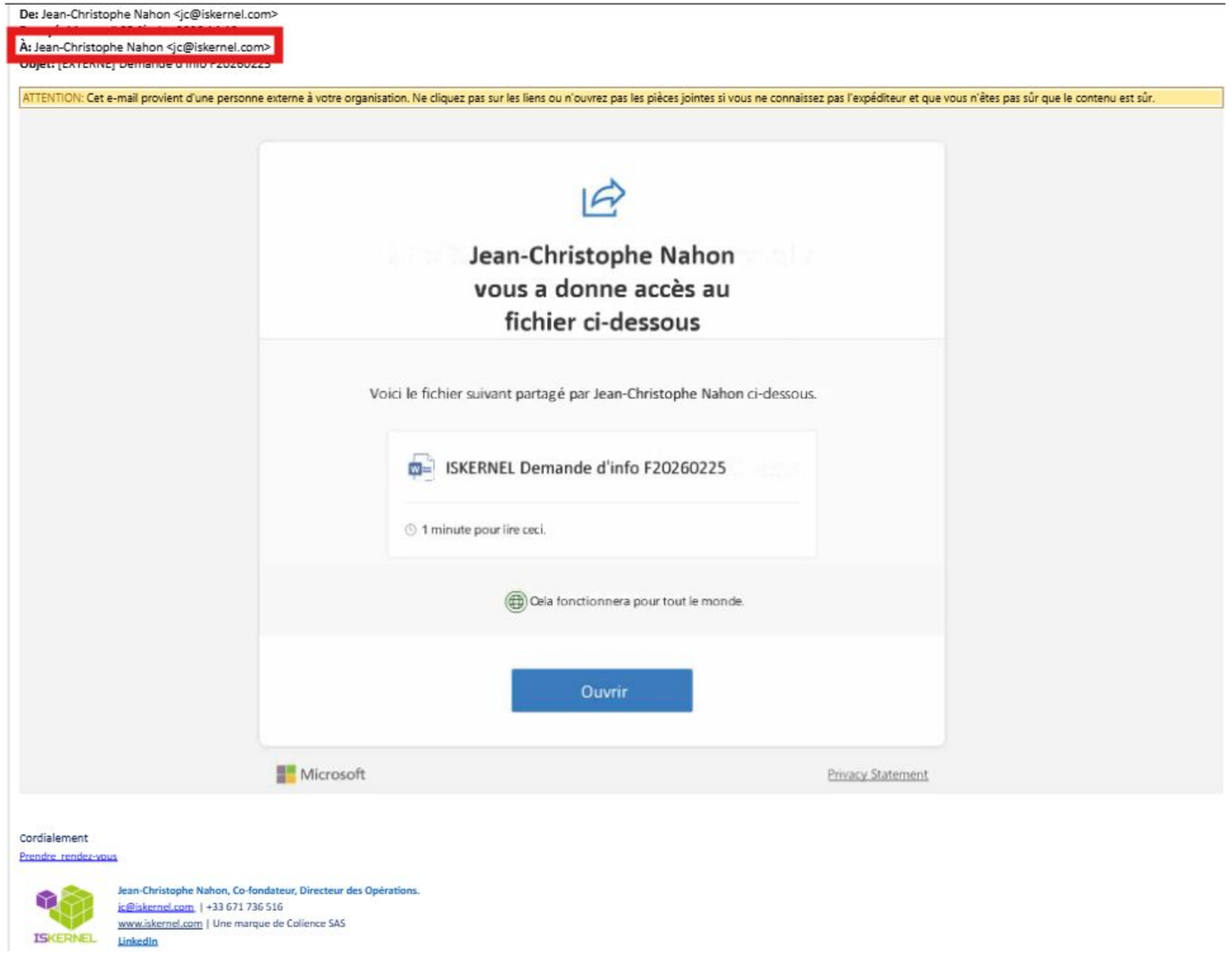
1) Nom d'expéditeur invalide. Attention, ce n'est pas un critère fiable à 100% car celui-ci peut être falsifié comme dans l'exemple.
2) Destinataire invalide : il doit correspondre à notre adresse email.
3) Texte du mail avec des fautes d'orthographe et une mauvaise mise en forme.
4) Lien HyperText vers un site piégé (passer la souris dessus sans cliquer pour voir le vrai lien).

COMMENT SE PROTÉGER

MENACES CYBER

COMMENT SE PROTÉGER

Email d’un contact ayant eu son compte compromis



L’arnaque au faux support

Un message apparaît sur l’écran en indiquant que le PC est infecté par un virus ou qu’il y a une erreur empêchant son utilisation. Un numéro de téléphone de faux support technique est affiché vous incitant à les appeler afin de réparer le poste.

Comment s’en protéger :

- Ne pas appeler le numéro affiché
- Appeler votre support informatique

L’arnaque au faux support par téléphone

Une personne vous appelle en se faisant passer pour quelqu’un du support afin de prendre la main sur le poste pour y installer des virus ou bien voler des données.

Comment s’en protéger :

- Vérifier via des sources fiables l’identité de l’interlocuteur (téléphone, voir la personne physiquement, etc…)

La fraude au président

L’arnaque au président consiste pour le fraudeur à se faire passer pour le président de la société. Le contact se fait par courriel ou par téléphone.

Après quelques échanges destinés à instaurer la confiance, le fraudeur demande la réalisation d'un virement international non planifié, au caractère urgent et confidentiel.

Comment s’en protéger :

- Vérifier via des sources fiables l’identité de l’interlocuteur (téléphone, voir la personne physiquement, etc…)

La fraude au faux RIB

L’arnaqueur se fait passer pour un fournisseur de l’entreprise et demande la modification des coordonnées bancaires pour recevoir les versements à la place du vrai fournisseur.

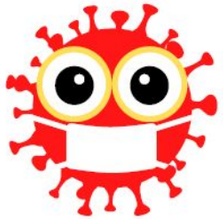
Comment s’en protéger :

- Ne pas agir dans la précipitation malgré l’insistance de l’interlocuteur
- Rappeler directement le fournisseur en passant par leur standard

MENACES CYBER

COMMENT SE PROTÉGER

MALWARE / CRYPTOLOCKER / VIRUS …



Programme informatique hostile qui, s'il réussit à s'installer, auto exécute des actions malveillantes sur le système informatique (virus, vers, cheval de
Troie, ransomware, etc.).

Comment s'en protéger :

- Mettre vos documents sur les lecteurs réseaux ou serveur qui sont sauvegardés (pas sur le bureau ou mes documents)
- Avoir un antivirus actif
- Ne pas naviguer et télécharger des logiciels sur des sites non professionnels
- Tenir à jour votre système

Que faire en cas de découverte d'une vulnérabilité ou d'une attaque ?

Tout problème de vulnérabilité ou attaque informatique doit être signalé à votre support informatique à l'adresse :
support@anamnese.care

Voici quelques des exemples de vulnérabilités/attaques :

- Répertoire sans droits d'accès appropriés (Dossier direction accessible par tout le monde)
- Faille dans un logiciel / Réseau (Wifi non sécurisé, Redirection de port etc..)
- Activité suspecte sur son poste (fichiers/processus/logiciels inconnus, souris qui bouge toute seule, etc..)
- Réception des mails de phishing
- Etc…


QUIZ!

QUIZZZZZZZ

Quel est la durée d’un cycle de l’ISO 27001 ?

A. Facile, c’est 3 ans

B. J’ai bien suivi la sensibilisation, je sais que c’est 1 an

C. Tout le monde le sait que c’est tous les 10 ans

QUIZZZZZZZ

Quel est le périmètre du SMSI ?

A. Les activités de Build, Run, Support et Hébergement de la plateforme SaaS

B. L'ensemble des services d'ANAMNESE, y compris le marketing et le commerce

C. Uniquement les infrastructures et les applications propres à nos clients

QUIZZZZZZZ

Que se passe t'il en cas de NC majeure ?

A. L'entreprise doit fermer jusqu'à ce que la NC soit corrigée

B. Nous devons corriger la NC dans les 2 semaines qui suivent l'audit

C. La certification nous est retirée immédiatement

QUIZZZZZZZ

Quelle est la longueur minimale à respecter dans un mot de passe utilisateur ?

A. 8 caractères, c’est amplement suffisant

B. 10 caractères, nous ne travaillons tout de même pas à la NASA

C. 12 caractères, comme les 12 travaux d’hercules

QUIZZZZZZZ

Puis je utiliser mon poste de travail pour une utilisation personnelle ?

A. Oui, c’est autorisé alors j’en profite !

B. Non, c’est trop risqué,

C. Oui, mais je ne dois pas me faire attraper

QUIZZZZZZZ

Puis je utiliser un poste d’un client hors de la France?

A. Non, Surtout pas !

B. Oui, pas de problème.

C. Oui, mais pas sans autorisation bien sur !

QUIZZZZZZZ

Quelle est la principale porte d’entrée des pirates ?

A. Ils utilisent des failles sur les serveurs web

B. Les mails de phishing

C. Ils se font embaucher par la société de ménage pour poser des appareils de hacking

QUIZZZZZZZ

Je reçois un mail douteux avec une pièce jointe, que dois je faire ?

A. Je contact le service support pour leur demander s’il est légitime

B. J’ouvre la pièce jointe, je verrai si cela me concerne

C. Je le transfère à Martine qui ne m’a pas laissé la dernière chocolatine

QUIZZZZZZZ

Je reçois un mail du directeur qui me demande de faire le transfert d'une grosse somme d'argent rapidement, que dois je faire ?

A. Je le fais car c'est le directeur et je dois faire tout ce qu'il me demande

B. Je le contact directement sur son numéro de téléphone connu pour m'assurer que la demande vienne bien de lui. En cas de non-réponse, je patiente

QUIZZZZZZZ

Je veux qu’une IA analyse un message d’erreur contenant des données techniques (IP, serveurs...), que dois-je faire au préalable ?

A. Je supprime toutes les données sensibles (IP, noms de serveurs...) avant d’utiliser l’IA.

B. ChatGPT avec sa fonction de raisonnement peut m’aider directement sans aucune modification préalable.

C. Je peux utiliser n'importe quelle IA publique, le chiffrement du transit garantit la confidentialité de mes données.

Anamnèse

Anticiper . Accompagner . Accélérer